IN THE DRAWINGS:

Please AMEND Figures 2A and 3A to replace “Hush Unit” with “Hash Unit.”

REMARKS

On page 2 of the Office Action, the drawings of the subject application were objected to because Figures 2A and 3A include the label "Hush Unit." As illustrated in the replacement drawing sheets attached hereto, Applicants have amended the drawings representing Figures 2A and 3A to change "Hush Unit" (element #2) to "Hash Unit," as suggested by the Examiner. Withdrawal of the objection is respectfully requested.

On page 3 of the Office Action, claims 27, 32, and 37-43 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,915,024 (Kitaori) in view of U.S. Pat. No. 6,009,524 (Olarig).

Kitaori is directed to an apparatus and method for adding an electronic signature to document data. According to Kitaori, the method includes dividing document data into a plurality of divided document data using as a delimiter a predetermined character appearing in a document represented by the document data, generating an electronic signature for each of the divided document data on the basis of the divided document data, and storing the divided document data, the electronic signature based on the divided document data, and information for associating the divided document data with the electronic signature. *See* Kitaori, column 4, lines 51-62.

Olarig discloses a system and method for FLASH BIOS upgrades. According to Olarig, each hub or node equipped with a FLASH memory is also equipped with a validation system, which ensures that a received FLASH upgrade is authorized and uncorrupted. Each set of instructions to be flashed is marked with a vendor authorization digital signature and a system administrator authorization digital signature. Before the FLASH memory will be upgraded, both digital signatures must be recognized by the validation system. Flash upgrades can be performed from any location on the network, that is, flash upgrades are not limited to an admin node, as digital signatures are used for security purposes.

The Examiner alleges that Kitaori discloses almost all of the features of claim 1. The Examiner further alleges, however, that Kitaori does not disclose, "using a different key and algorithm to create a one-way hash on each of the divided data."

The Examiner alleges that Olarig teaches using two different signatures with different keys on data.

In light of the foregoing, Applicants respectfully submit that independent claims 27, 32, and 37-43 are patentable over the references, as neither of the references, taken alone or in combination, teaches or suggests, ". . .applying a first one-way function using a first key to each of the data divisions" and ". . .applying a second one-way function using a second key to each of the data divisions," as recited in independent claim 27, for example.

Beginning at column 8, line 5, Kitaori discloses a digest generator that applies "a" hash function to a signature message to generate a message digest. Although Kitaori discloses that the hash function is predetermined, only one hash function is applied in Kitaori. *See* Kitaori, column 8, lines 5-17 (stating throughout that "a" hash function is used). Therefore, Kitaori does not disclose or suggest applying a first one-way function *and* a second one-way function. Moreover, Kitaori does not indicate whether the hash function is a one-way function.

Similarly, Olarig does not teach or suggest, ". . .applying a first one-way function using a first key to each of the data divisions" and ". . . applying a second one-way function using a second key to each of the data divisions," as recited in independent claim 27, for example. Rather, Olarig merely discloses the attachment of an authorization digital signature. Assuming *arguendo* (solely for the purpose of argument) that attachment of the authorization digital signature is accomplished by a one-way function, Olarig does not disclose applying a second one-way function, as the vendor's key is merely used for verification purposes.

In light of the foregoing, neither Kitaori nor Olarig, taken alone or in combination, teaches or suggests, ". . .applying a first one-way function using a first key to each of the data divisions" and ". . . applying a second one-way function using a second key to each of the data divisions," as identified by the independent claims of the present invention.

On page 4 of the Office Action, claims 28 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kitaori in view of Olarig in view of U.S. Pat. No. 6,023,509 (Herbert).

Although Herbert creates a digital signature, the data to be signed is passed through one single hash function. Therefore, Herbert does not teach or suggest, ". . . applying a first one-way function using a first key to each of the data divisions" and ". . . applying a second one-way function using a second key to each of the data divisions." *See* Herbert, column 3, lines 1-7. *See also* Herbert, FIG. 1 (illustrating the passing of data 100 through a sole hash function 200).

Therefore, claims 28 and 33, via independent claims 27 and 32, respectively, are patentable over the references, as none of the references, taken alone or in combination, teach or suggest the above-identified features of the claims of the present invention.

On page 5, claims 29, 31, 34, and 36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kitaori in view of Olarig in view of U.S. Pat. No. 5,604,801 (Dolan).

Dolan merely creates a digital signature by using a single hashing function. Therefore, Dolan does not teach or suggest ". . .applying a first one-way function using a first key to each of the data divisions" and ". . . applying a second one-way function using a second key to each of the data divisions," as identified by the independent claims of the present invention. Hence, claims 29, 31, 34, and 36, via independent claims 27 and 32, are patentable over the references.

On page 6 of the Office Action, claims 30 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kitaori in view of Olarig in view of U.S. Pat. No. 5,757,913 (Bellare).

Although Bellare discloses that a pseudo-random function is applied to a word, Bellare does not disclose that the pseudo-random function is a one-way function. Moreover, Bellare does not disclose that a key is used, as in the present invention. Further still, Bellare only discloses one pseudo-random function. *See* Bellare, column 2, lines 1-17.

Therefore, claims 30 and 35, via claims 27 and 32, respectively, are patentable over the references, as none of the references, taken alone or in combination, teach or suggest the above-identified feature of the present invention.

Applicants respectfully submit that claim 45 is patentable over the references, as none of the references, taken alone or in combination, teach or suggest, "applying one-way functions to the data to create a first authenticator and a second authenticator; and appending the first and second authenticators to the data."

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of the present response, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 2/28/06

By:
Reginald D. Lucas
Registration No. 46,883

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501